Abstract

A method and system are directed to differentiating between normal characteristics and abnormal characteristics within a software process, such that tampering of the software process may be identified programmatically. The identification of behavior that may be defined as normal may vary. Such behavior may include a sequence of selected system level calls that may access resources considered relevant, and the like. Data on the selected behavior is gathered, and when a sufficient amount of abnormal behavior has been detected, a signal may be provided such that an action may be performed. Samples of the gathered data are assigned a unique value. Statistical information is determined from the collected behavior, including trend data. Such trend data is compared to trends identified as normal for the software process, and a determination is made whether the sampled behavior is non-normal.

Customer No.: 07278